Statement of Melissa Smislova, Director
Homeland Infrastructure Threat and Risk Analysis Center
US Department of Homeland Security
before the
House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment

"Private Sector Information Sharing: The DHS Perspective and Lessons Learned"

July 26, 2007

Introduction

Good morning, Chairwoman Harman, Ranking member Reichert, and distinguished Members of this Subcommittee. I welcome the opportunity to speak again to this subcommittee on the progress of the Department of Homeland Security in sharing intelligence information with the private sector. I will also take this time to discuss the lessons we have learned during our outreach and inform you of our plans to improve information sharing.

I manage both the Department's joint program office for assessing the risk to the critical infrastructure and key resources of the United States, known as the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), as well as the DHS Office of Intelligence and Analysis (I&A), Critical Infrastructure Threat Analysis Division (CITA), which supports HITRAC as its discrete, embedded intelligence component. Through my involvement with HITRAC and CITA, I am able to oversee the collocation of DHS intelligence analysts with the Department's infrastructure protection experts responsible for performing sector-specific risk assessments. The virtue of maintaining CITA's existence as a separate albeit embedded threat unit within HITRAC ensures that all intelligence production remains subject to the oversight and policies of the Department's Assistant Secretary for Intelligence and Analysis and Chief Intelligence Officer.

Production

Since I last testified to this subcommittee in November 2005 significant progress has been made in developing and disseminating products and

briefings tailored specifically for the private sector audience. In that time, HITRAC/CITA has produced over 171 separate products for critical infrastructure protection analysts in the private sector, State and local homeland security agencies, and the law enforcement community. Of these, 40 were assessments jointly written and published with the Counter Terrorism Division of the Federal Bureau of Investigation.

We have also systematically and routinely conducted classified and unclassified intelligence briefings for the private sector, largely through the National Infrastructure Protection Plan Partnership Model, but also through our discrete relationships with industry associations, our attendance at conferences, and outreach directly to individual private sector entities.

While I am proud of our accomplishments and I believe the work done so far creates a good baseline, I do know that much work remains. As our relationship grows with the private sector and with the critical infrastructure community in State and local governments, we are increasingly learning about new requirements. The information needs of the private sector and of the States are diverse, and we are challenged to create products and briefings to meet them.

One of the first lessons we learned was that private sector and the critical infrastructure protection officials in State and local law enforcement community's work closely together yet sometimes have different information requirements. We began our HITRAC/CITA production efforts with assessments aimed at addressing known and potential threats to sectors – or systems - of like critical infrastructure. While we found that those products were well received by some our private sector customers, States were more interested in regionally focused analyses. We have responded by expanding our product lines and outreach efforts to address, in addition to core sector specific concerns, the broader, cross-sector regional issues.

Intelligence Information Designed for the Private Sector

We produce classified assessments and do regularly give classified briefings to members of the private sector. The Department of Homeland Security and FBI have sponsored many of our customers for clearances to receive classified information. We also disseminate these assessments at various classification levels, modified, of course, to adhere to all applicable

classification rules and other requirements for protecting sensitive information, but with the goal of reaching as many customers as possible.

However, our interaction with the private sector has underscored their interest in the details of intelligence reports vice source information. Much of what makes a report classified is its reference to collection. Because of that focus we have been very successful in working with the intelligence community to ensure the downgrading of key information on terrorist tactics, techniques and procedures. Many of our products use information we have first worked to downgrade from classified to unclassified.

Another lesson learned was that many within the critical infrastructure information sharing community were interested in reporting about numerous sectors. Thus, we expanded dissemination.

Our product lines now respond to what we have gathered about private sector needs and continue to evolve with private sector involvement. We continually reach out to a broad spectrum of private sector representatives to refine the scope of our assessments, and have come to learn that private sector information requirements are not only numerous, but have become more complex as our private sector partners have become more knowledgeable about intelligence and terrorism generally. Thus, where in the beginning many of our products summarized merely what was known about existing terrorists' interest in certain types of infrastructure as potential targets, our product lines now reflect our customers expanded interests in more detailed analysis of terrorist tradecraft, including especially surveillance techniques and attack methods.

Many of our products have benefited from the insight and, in many cases, direct input of members of the private sector as those products are being developed. In addition, this direct interaction with the private sector has also assisted the Department in clarifying, or putting into better context, vague or incomplete threat reporting.

Some of our current product lines include:

- ***Quarterly and Annual Suspicious Activity Assessment (SAA):*** These assessments provide strategic, national-level analysis of suspicious incidents reported to DHS. They use information provided by the private sector and are an attempt to provide industry with trend and

pattern analysis of incidents noted at their facilities. This represents a genuine and valued partnership between the government and private industry.

With the direct involvement and knowledgeable support of the private sector, we have been able to establish a baseline of "suspicious activity" reflected in these assessments. For example, when we recently received reports that electrical power towers were possibly being sabotaged, private sector electrical industry professional familiar with that particular region suggested to us that the activity was more likely illegal, albeit non terrorist related, tampering often seen in that area of the country during hunting season – i.e., elements of the power towers are used illegally to create deer blinds. Similarly, we believe we have been able to better educate the private sector about terrorist surveillance techniques and alert them when suspicious activity might indicate pre-operational terrorist activity.

- **CINT Notes –** In conjunction with notes regularly sent out by the Chief Intelligence Officer, Charlie Allen, concerning current threat activities or information, we communicate directly with all stake-holders, including the private sector, to inform them of what we know about incidents as they unfold. CINT notes and follow up coordination with relevant partners concerning the recent attempted attacks in London and Glasgow is a good example of this means for sharing pertinent information.

  Mr. Allen also makes direct phone calls to US companies if they are specifically mentioned in intelligence reporting.

- ***Infrastructure Intelligence Note (IIN)*** – Generally a short product that provides the infrastructure owners and operators and State and local partners with a timely perspective on events, activities, or information of importance to support security planning. These products differ from the CINT notes in that they entail more research and time to craft. Some Infrastructure Intelligence Notes are generated directly by calls from private industry based upon specific sector questions or concerns. We also use the Infrastructure Intelligence Note to discuss lessons learned from terrorists' attacks overseas. These assessments are provided to enhance our critical infrastructure protection

community's understanding of evolving terrorist tactics, techniques, and procedures.

- ***Joint Homeland Security Assessment*** – Products written with the Counter Terrorism Division of the Federal Bureau of Investigation. These assessments communicate intelligence information that affects the security of U.S. citizens or infrastructure. Provides information on training, tactics, or terrorist strategies, and analyzes incident trends and patterns. This product also may recommend protective measures. During the last two years we have built a valued and productive relationship with our colleagues at the FBI. This partnership not only produced more comprehensive assessments, but ensures that the government speaks with one voice to our customers.

- ***Strategic Sector Assessments*** – These were our first unique HITRAC products and were intended to provide a baseline analysis of the threats and risks to the entire critical infrastructure. These products are written at multiple classification levels, detail our analysis of the intentions and capabilities of known terrorists, and integrate relevant threat information. Some of the sector-specific assessments include discussion of the unique vulnerabilities and consequences unique to that sector.

- ***State and Regional Threat Assessments*** – As I mentioned, one of our lessons learned is that elements of the critical infrastructure community are interested in regionally focused assessments. This is an area of production we are working on with the support of private sector and State partners. While we have created several regional assessments, our efforts are in the beginning stages.

Lessons Learned and Future Opportunities

We continue to modify our processes and products based on customer feedback and other lessons learned. We believe these modifications have made us more responsive to our stakeholders and have enabled us to create better products.

Integration with State and Local governments.

While our initial efforts were focused on the CI/KR owners and operators, we have dramatically increased our work for and with State and local authorities who have significant responsibilities for security, risk mitigation and incident response around the nation CI/KR.

We now have an aggressive outreach plan that includes State and local as well as private sector critical partners to identify information needs and to tailor analyses and products to meet these requirements. As part of this outreach plan, we are regularly meeting with Homeland Security Advisors and their staffs to integrate State information and their analysis into the creation of state critical infrastructure threat assessments. By doing this we hope to gain a more comprehensive appreciation for the threats in the states.

Specific Outreach initiatives. We initiated and continue to participate in weekly conference calls with multiple critical infrastructure sectors as well as an analytic exchange between DHS intelligence analysts and State and Local Fusion Centers.

Conclusion

In conclusion, I believe partnering intelligence professionals with sector experts and security personnel has proven successful for developing better threat assessments. I believe we have made significant progress developing product lines and briefings that provide tailored intelligence information to the private sector, States and law enforcement communities.

We are excited about improving our analytic understandings of the various threats to critical infrastructure. We understand that working in partnership with the private sector, States, and local governments is the way to achieve that improvement. Our goals for the future include enhancing our regionally focused assessments and better integrating vulnerability and consequence data into our analysis.

Thank you.